Ministry of Education and Science of Ukraine

Odessa National Academy of Food Technologies

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2021

Information Technology, Automation and Robotics

Proceedings

Odessa, ONAFT 2021

UDC 004.01/08

Editorial board:

Black Sea Science 2021: Proceedings of the International Competition of Student Scientific Works. Information Technology, Automation and Robotics. / Odessa National Academy of Food Technologies; B.Yegorov, M. Mardar, S.Kotlyk (editors-in-chief.) [*et al.*]. – Odessa: ONAFT, 2021. – 526 p.

These materials of International Competition of Student Scientific Works «Black Sea Science 2021» contain the works of the contest participants in the section «Information technologies, automation and robotics» (not winners).

The author of the work is responsible for the accuracy of the information.

Organizing committee:

Prof. Bogdan Iegorov, D.Sc., Rector of Odessa National Academy of Food Technologies, Head of the Committee

Prof. Maryna Mardar, D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations of Odessa National Academy of Food Technologies, Deputy Head of the Committee

Prof. Stefan Dragoev, D.Sc., Vice-Rector for Scientific Work and Business Partnerships of University of Food Technologies (Bulgaria)

Prof. Baurzhan Nurakhmetov, D.Sc., First Vice-Rector of Almaty Technological University (Kazakhstan)

Prof. Mircea Bernic, Dr. habil., Vice-Rector for Scientific Work of Technical University of Moldova (Moldova)

Prof. Jacek Wrobel, Dr. habil., Rector of West Pomeranian University of Technology (Poland)

Prof. Michael Zinigrad, D.Sc., Rector of Ariel University (Israel)

Dr. Mei Lehe, Ph.D., Vice-President of Ningbo Institute of Technology, Zhejiang University (China)

Prof. Plamen Kangalov, Ph.D., Vice-Rector for Academic Affairs of "Angel Kanchev" University of Ruse (Bulgaria)

Dr. Alexander Sychev, Ph.D., Assoc. Professor of Sukhoi State Technical University of Gomel (Belarus)

Dr. Hanna Lilishentseva, Ph.D., Assoc. Professor, Head of the Department of Merchandise of Foodstuff of Belarus State Economic University (Belarus)

Prof. Heinz Leuenberger, Ph.D., Professor of the Institute of Ecopreneurship of University of Applied Sciences and Arts (Switzerland)

Prof. Edward Pospiech, Dr. habil., Professor of the Institute of Meat Technology of Poznan University of Life Sciences (Poland)

Prof. Lali Elanidze, Ph.D., Professor of the Faculty of Agrarian Sciences of Iakob Gogebashvili Telavi State University (Georgia)

Dr. V. Kozhevnikova, Ph.D., Senior Lecturer of the Department of Hotel and Catering Business of Odessa National Academy of Food Technologies, Secretary of the Committee

The jury for the section «Information technologies, automation and robotics»

Head of the jury:

Sergii Kotlyk – Ph.D., Associate Professor, Director of the P.M. Platonov Educational-Scientific Institute of Computer Systems and Technologies "Industry 4.0" of Odessa National Academy of Food Technologies (Ukraine)

Members of the jury:

Piotr Artiemjew - Dr hab., Associate Professor in Decision Systems of the Faculty of Mathematics and Computer Science,University of Warmia and Mazury in Olsztyn (Poland)

Francisco Antonio Augusto – Dr., International Relations Manager of Higher Institute of Information and Communication Technologies (Angola)

Andrey Kuprijanov – Ph.D., Associate Professor of the Department of Software for Computers and Automated Systems of Belarusian National Technical University (Belarus)

Simon Milbert – Vice-President of Xtra Information Management, Inc. (USA)

Ivan Palov – D.Sc., Professor of University of Ruse "Angel Kanchev" (Bulgaria)

Degla Gérard Hugues – Communications and Training Manager of "MAPCOM solutions informatiques" company group (Benin)

Nugzar Kereselidze - Academic Doctor of Informatics (Computer Science), Associate Professor of the Department of Natural Sciences, Mathematics, Technology and Pharmacy, Sukhumi State University (Georgia)

Etibar Seyidzade - Associate Professor of the Department of Computer and Information Technolohies, Baku Engineering University (Azerbaijan)

Vladimir Golenkov, D.Sc., Professor of the Department of Intelligent Information Technologies, Belarusian State University of Informatics and Radio Electronics (Belarus)

Zhanar Omirbekova - Ph.D., Associate Professor of the Department of Automation and Management, Satbayev University (Kazakhstan)

Ivan Palov - D.Sc., Professor of the Department of Power Supply and Electrical Equipment, University of Ruse "Angel Kanchev" (Bulgaria)

Siarhei Palavenia - Ph.D., Associate Professor, Head of the Department of Telecommunication Systems, Belarusian State Academy of Communications (Belarus)

Alexander Goloskokov - Ph.D., Professor of the Department of Software Engineering and Information Technology Management, National Technical University "Kharkiv Polytechnic Institute" (Ukraine)

Peter Nikolyuk - D.Sc., Professor of the Department of Computer Technology, Vasyl Stus Donetsk National University (Ukraine)

Vladimir Palagin - D.Sc., Professor, Head of the Department of Radio Engineering, Telecommunications and Robotics Systems, Cherkasy State Technological University (Ukraine)

Viktor Khobin – D.Sc., Professor, Head of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies (Ukraine)

Valeriy Plotnikov – D.Sc., Professor, Head of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

Sergii Artemenko – D.Sc., Professor, Head of the Department of Computer Engineering of Odessa National Academy of Food Technologies (Ukraine)

Fedir Trishyn - Ph.D., Associate Professor, Vice-Rector on Scientific and Educational Work, Odessa National Academy of Food Technologies (Ukraine)

Valerii Levinskyi – Ph.D., Associate Professor of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies (Ukraine)

Viktor Yehorov – Ph.D., Supervisor of the Laboratory of Mechatronics and Robotics of Odessa National Academy of Food Technologies (Ukraine)

Pavlo Lomovtsev – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

Yurii Kornienko – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

Serhii Shestopalov – Ph.D., Associate Professor of the Department of Computer Engineering of Odessa National Academy of Food Technologies (Ukraine)

Anatoly Galiulin - Ph.D., Associate Professor, Acting Head of the Department of Electromechanics and Mechatronics, Odessa National Academy of Food Technologies (Ukraine)

Secretary of the jury:

Oksana Sokolova – Senior Lecturer of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

2.RBK.(2017, December 17). How Disney created the first feature-length cartoon [Video]. YouTube. https://www.youtube.com/watch?v=-8LiVIufw4k

3. Prajwal K.R., Rudrabha Mukhopadhyay, Namboodiri V. P., Jawahar C.V. (2020). A Lip Sync Expert Is All You Need for Speech to Lip Generation In the Wild. https://arxiv.org/pdf/2008.10010.pdf

4. Prajwal K.R, Rudrabha Mukhopadhyay, Jerin Philip, Abhishek Jha, Vinay Namboodiri, Jawahar C.V. (2019) Towards Automatic Face-to-Face Translation https://dl.acm.org/doi/10.1145/3343031.3351066

5. Deepali Aneja, Wilmot Li (2019). Real-Time Lip Sync for Live 2D Animation https://arxiv.org/pdf/2008.10010.pdf

6. Medvedev M.S. (2004). Phone segmentation of a speech signal using a wavelet transform http://www.ict.nsc.ru/ws/YM2004/8614/Medvedev.html

CYBERSECURITY AS A METHOD OF COMBATING UNAUTHORIZED INFLUENCE IN THE FIELD OF INFORMATION SECURITY

Author: ***Ilia Burykin***
Advisor: ***Iryna Muntian***
Professional College of Industrial Automation and Information Technologies of the Odessa National Academy of Food Technologies (Ukraine)

Abstract: *The article describes the main problems, the protection of user's data, methods of combating unauthorized impact in the field of information security. Comparison of antivirus programs.*

This work demonstrates that at the moment there are still many people who can be cyberattacked in obtaining important information.

Keywords: *cybersecurity, password, protection, data, hacking, phishing, antivirus.*

I. INTRODUCTION

Today we cannot imagine our life without technologies. They have flooded the world, helping, entertaining, educating us. Almost everyone has his own smartphone, laptop or computer, which contains confidential information. But many of us make mistakes that can cause to obtaining that information, by third persons. Just then we think of cybersecurity. It has become an important component of our digital lives.

Unfortunately, every year some of the most popular passwords make it to the top are: 123456, 123456789, qwerty and so on (full list[1]). This means that many devices are exposed to threats of hacking and obtaining confidential information. At the same time, everyone knows not to use easy passwords, and many sites and applications are already prompting about the security of the passwords entered, and are trying to prevent logging in with simple passwords. Also one of the most popular ways of obtaining data is phishing, which is a type of Internet scam aimed at gaining

access to confidential user data. Namely, these are fake emails, links from famous brands whose aim is to lead you to a site that is virtually indistinguishable from the original.

Also, don't forget that you may not be a specific user for the hack, but only a bridge to the main target. Protection of a community of people is much more complicated than a simple computer password. You may be endangering the company where you work, your friends, your family. So it's worth to paying attention to your cybersecurity situation, your devices, your accounts, and fix it as soon as possible, get efficient knowledge, and skills in this area.

II. LITERATURE ANALYSIS

Cybersecurity is the activity aimed at systems protection, networks and programs against digital attacks. The purpose of such cyber attacks is usually to gain access to confidential information, alter or destroy it, extort money of users, or disrupt normal business processes. [5]

Types of cybersecurity threats:

1.*Phishing*is sending of fake emails that look like messages from trusted recipients. The purpose of this type of fraud is to steal sensitive data, such as credit card numbers and credentials. [5] This is the most common type of cyberattack. You can protect yourself from phishing by using user education or a solution that blocks malicious emails. For example, fakebook.com or faecbook.com or any other URL that is very similar to the original one. When a user visits such a page, he might not pay attention to the wrong page address because of the similarity of the page address to the original one. And may take this phishing page as a real Facebook login page and use the login form without any fear. [6]

2. *Ransomware* is a type of malware. They extort money by blocking access to files or computer systems until a ransom is paid. [5] Paying a ransom does not guarantee access to the files or that systems will be restored. For example, Petya, an attack using the encryption virus Petya (not to be confused with ExPetr) was detected in 2016, and in 2017 the attack was repeated as GoldenEye. Petya encrypts not the files themselves, but the victim's entire hard drive. It does this by encrypting the MFT table, a database with information about all the files stored on the disk, making it impossible to access the files. Petya gets on the PC "pretending" to be a letter to HR from a candidate for this or that position. The HR professional receives a fake email with a link to Dropbox, which he supposedly can go to and download the "resume." [7]

3. *Malware* is a software designed to gain unauthorized access to a computer or cause damage. [5] Examples of malware:[8]

- viruses;
- macro viruses for Word and Excel;
- boot viruses; script viruses, including batch viruses that infect Windows shells, Java applications, etc;
- keyboard spies;

- password stealing software;
- backdoor Trojans;
- Crimeware is a malware designed to automatize the commission of financial crimes;
- spyware;
- adware and other types of malware

4. *Social engineering* is used by cybercriminals to trick you into revealing sensitive information. They might ask you to make a money transfer or give you access to sensitive data. Social engineering can be combined with any of the above mentioned types of threats to make you more likely to click links, download malware, or trust a malicious source. [5] An example of taking advantage of social engineering (an example of a competent social engineer). An intruder needs to get some amount of money from you. Suppose he found your cell phone and social network. Doing a search on the Internet, he also found that you have a brother. He found his social network and started looking into it to get into his way of thinking. He also found his cell phone for insurance and opened his correspondence, where he found messages with you. He studied them and learned various personal facts about you, which he added to his awareness after looking at your social media. Then a plan was made, which included the following: the abuser calls you late at night and pretends to be your brother, saying that he had his head bashed in and was thrown out somewhere in the street, his phone stolen as well as all the money with the cards (so he justifies why someone else's number is calling you). It is important that he addressed you not by name, but by the nickname he saw in your personal correspondence - this is a very important point. Next, for plausibility, he says, for example, that he was sitting with some of your common friends in a place you often go to - a bar, a club, whatever (photos and geo-references to help). Next, after such a story, he says that the main thing is not to tell his parents! My father has ill health (found out from the hacked dialogue). After that, goes by something like: "Throw me 500 grn for a cab to the hospital" - and gives his card number, saying that there was a kind girl who helped him, only she has no money, but the card. In 8 cases out of 10 after such a competent approach, our fictional sister will transfer the money, and then from her account all the money will be withdrawn, not just 500grn. For a technically competent hacker this is not a problem at all. [3]

5. A *denial-of-service attack* (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Another way of understanding DDoS is seeing it as attacks in cloud of computing environment that are growing due to the essential characteristics of cloud computing. Although the means of carrying out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts to prevent an Internet site or service from functioning efficiently, temporarily or indefinitely. According to businesses who participated in an international business security survey, 25% of respondents experienced a DoS attack in 2007 and 16.8% experienced one in 2010. DoS attacks often use bots (or a botnet) to carry out the attack. [9]

Antivirus program (antivirus) - any program for detecting computer viruses, as well as undesirable (considered as malicious) programs in general and restoring files infected (modified) by such programs, as well as for prevention - preventing the infection (modification) of files or the operating system by malicious code. [10]

A cyberattack is a malicious, deliberate attempt of a person or organization to penetrate into the information system of another person or organization. As a rule, by disrupting the victim's network, the hacker seeks to gain profit. [12]

Internet security is a branch of computer security specifically related not only to Internet, often involving browser security and the World Wide Web, but also network security as it applies to other applications or operating systems as a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information, which leads to a high risk of intrusion or fraud, such as phishing, online viruses, trojans, worms and more. [11]

III. OBJECT, SUBJECT, AND METHODS OF RESEARCH

The purpose of the research of this paper: to make people aware of the problem of cybersecurity, in order to reduce the acquisition of confidential information by third persons. The main methods to help you to protect your data.

Object of study: different methods of unauthorized access to data.

Subject of study: various devices (laptop, phone, PC), accounts.

IV. RESULTS

Basic data protection methods:[13]

The currently known general methods for ensuring information security consist of organizational and technical, economic and legal methods. Organizational and technical methods of information security (IS) include:

- information security system (by this we mean a set of measures (internal rules for work with data, regulations of data transfer, access to them, etc.) and technical means (the use of programs and devices to maintain data confidentiality));
- development (creation of new), operation and improvement of existing means of information protection;
- permanent control over the effectiveness of measures taken in the field of information security.

The last point is particularly important. Without an evaluation methodology, it is very difficult to determine the effectiveness of the IS. If the efficiency drops, it is necessary to take urgent make adjustments (this is what permanent control is for).

Information security is always a complex system, all components of which are designed to prevent the leakage of confidential information through technical channels, as well as to prevent unauthorized access to data carriers. Respectively, all this, guarantees the integrity of data during its handling: processing, transmission and storage, which should be carried out compulsory in the legal field. Being competently organized technical measures allow to determine the use of special electronic devices

of unauthorized removal of information, placed both in the premises and in the means of communication.

Fig. 1: Stages of IS provision at the enterprise

The main rules of a successful information security system:

- permanence of the action of the established rules;
- completeness of the measures taken;
- comprehensiveness;
- consistency;
- effectiveness.

To ensure the information security of data stored and transmitted by technical means:

- authentication;
- regulate access to objects;
- encrypting file system;
- keys; secure connections;
- Ipsec are used.

Let's dwell on each of these forms of information security in more detail. All users of operating systems have encountered such an element of information security as login and password. This is authentication. It is the most common way to ensure data security, including information messages stored on a server or PC. Regulating access to objects (folders, files stored in the system) may also be based on authentication, but other algorithms are often used (the system administrator defines rights and privileges, according to which they can either familiarize themselves with certain objects, or, besides familiarization, make changes to them, or even delete them). File encryption (another component of information security) is performed by the EFS system using a key. Speaking of ensuring secure connections, information channels of the "client-client" or "client-server" type are used for this purpose. This method of information security is widely used in the banking sector. And to conclude about IPsec. This is a set of protocols for ensuring information security of data transmitted over IP.

Methods of protection

In practice, several groups of protection methods are used, namely:

- an obstacle on the way of an alleged kidnapper, created by physical and software means;
- control, or influence on the elements of the protected system; masking, or transformation of data, usually by cryptographic means;

- regulation, or the development of regulations and a set of measures designed to encourage users interacting with databases to behave properly;
- constraint, or the creation of such conditions in which the user will be forced to comply with the rules of data handling;
- inducement, or the creation of conditions that motivate users to behave in a proper way.

Each of the methods of information protection is implemented by different categories of means. The main means are organizational and technical.

Organizational protection of information[14]

The development of a set of organizational means of information protection should be in competence of the security service. Most often, security specialists:

- develop internal documentation that establishes the rules for working with computer equipment and confidential information;
- conduct briefings and periodic inspections of personnel;
- initiate the signing of additional agreements to employment contracts that specify the responsibility for the disclosure or misuse of information that has become known through work;
- delineate areas of responsibility to avoid situations where arrays of the most important data are an the disposal of one employee;
- organize work in common workflow programs and make sure that critical files are not stored off network drives;
- implement software products that protect data from being copied or destroyed by any user, including the organization's top management;
- make plans to recover the system in case it fails for any reason.

If a company does not have a dedicated IS service, it can invite to a security an outsourcing specialist. A remote employee will be able to audit the company's IT infrastructure and make recommendations for its protection from external and internal threats. Outsourcing in IS also implies the use of special programs for the protection of corporate information.

Technical means of information protection

The group of technical means of information protection combines hardware and software. The basic are:

- backup and remote storage of the most important data arrays in the computer system - on a regular basis;
- duplication and redundancy of all network subsystems that are important for data preservation;
- Creating the ability to reallocate network resources in cases of malfunction of individual elements;
- ensuring that backup power systems can be used; ensuring safety against fire or water damage of the equipment;
- installation of software that protects databases and other information from unauthorized access.

The set of technical measures also includes measures to ensure the physical

inaccessibility of computer network objects, such as practical methods of equipping the room with cameras and alarms.

Authentication and identification[14]

To prevent unauthorized access to information, methods such as identification and authentication are used.

Identification is a mechanism of assigning one's own unique name or image to a user who interacts with information.

Authentication is a system of ways to verify that a user matches the image to which access is granted.

These tools aim to grant or, conversely, deny access to the data. Authenticity, as a rule, is defined in three ways: program, machine, person. In this case, the object of authentication can be not only a person, but also a technical means (computer, monitor, media) or data. The simplest way of protection is a strong password.

Comparison of antivirus programs

According to AV-Test Labs, 2020 conducted comprehensive anti-virus testing[4]:

Manufacturer	Product	AV-TEST-Certificate	Protection (max. 6 pts.)	Performance (max. 6 pts.)	Usability (max. 6 pts.)	Total Score (max. 18 pts.)
AhnLab	V3 Internet Security	TOP	6.0	6.0	5.5	17.5
Avast	Free Antivirus		5.5	5.5	6.0	17.0
AVG	Internet Security		5.5	5.0	6.0	16.5
Avira	Antivirus Pro	TOP	5.5	6.0	6.0	17.5
Bitdefender	Internet Security	TOP	6.0	6.0	5.5	17.5
BullGuard	Internet Security	TOP	6.0	6.0	5.5	17.5
ESET	Smart Security		5.5	5.5	6.0	17.0
F-Secure	SAFE	TOP	6.0	6.0	6.0	18.0
G Data	Internet Security		5.5	5.5	5.0	16.0
K7 Computing	TotalSecurity		5.5	6.0	5.5	17.0
Kaspersky	Internet Security	TOP	5.5	6.0	6.0	17.5
Malwarebytes	Premium		4.0	4.0	4.5	12.5
McAfee	Total Protection		5.0	6.0	6.0	17.0
Microsoft	Defender		5.5	5.5	6.0	17.0
Microworld	eScan internet security suite		3.0	6.0	5.5	14.5
NortonLifeLock	Norton 360	TOP	6.0	5.5	6.0	17.5
PC Matic	PC Matic		5.5	6.0	3.0	14.5
Protected.net	Total AV		5.0	5.0	6.0	16.0
Trend Micro	Internet Security	TOP	6.0	6.0	6.0	18.0
VIPRE Security	AdvancedSecurity		5.5	6.0	5.5	17.0

Fig. 2.Comparison of antivirus programs

The symbols on the graph:

- Protection - the level of antivirus protection.
- Performance - the capacity of the application.

- Usability is a usability parameter, which is evaluated by the level of false positives.

V. CONCLUSIONS

The paper describes the main methods of unauthorized access to data, unfortunately, the list of methods is growing every year, but also cybersecurity does not stand behind and every year is improving. Everyone can increase his own security, the basic requirements:

- Update your software and operating system. Using new software, you get the latest security patches.
- Use antivirus programs. Security solutions, such as Kaspersky Total Security, can help identify and eliminate threats. For maximum security, update your software regularly.
- Use strong passwords. Do not use combinations that are easy to pick or guess.
- Do not open email attachments from unknown senders - they may be infected with malware.
- Do not click on links received in the mail from unknown senders or unknown websites - this is one of the standard ways malware spreads.
- Avoid unsecured Wi-Fi networks in public places, where you are vulnerable to Man-in-the-Middle attacks.

VI. REFERENCES

1. The most popular passwords. [Electronic resource]: Access mode: URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D0%B8#.2A2020:_.D0.9D.D0.B0.D0.B7.D0.B2.D0.B0.D0.BD.D1.8B_.D1.81.D0.B0.D0.BC.D1.8B.D0.B5_.D0.BF.D0.BE.D0.BF.D1.83.D0.BB.D1.8F.D1.80.D0.BD.D1.8B.D0.B5_.D0.BF.D0.B0.D1.80.D0.BE.D0.BB.D0.B8_.D0.B2_2020_.D0.B3.D0.BE.D0.B4.D1.83
2. Internet security [Electronic resource]: Access mode: URL: https://en.wikipedia.org/wiki/Internet_security
3. Example Social Engineering [Electronic resource]: Access mode: URL: https://emisare.medium.com/socialnaya-ingeneria-9f16e0ba7fa5
4. AV-Test 2020 [Electronic resource]: Access mode: URL: https://www.comss.ru/page.php?id=6963
5. What is cybersecurity? [Electronic resource]: Access mode: URL: https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html
6. Пример фишинга[Electronic resource]: Access mode: URL: https://hetmanrecovery.com/ru/recovery_news/what-is-phishing-overview-and-examples.htm
7. Example ransomware viruses [Electronic resource]: Access mode: URL: https://www.kaspersky.ru/resource-center/threats/ransomware-examples
8. Example malware [Electronic resource]: Access mode: URL: https://www.kaspersky.ru/resource-center/preemptive-safety/faq
9. Denial-of-service attack (DoS attack) [Electronic resource]: Access mode: URL: https://en.wikipedia.org/wiki/Denial-of-service_attack#:~:text=In%20computing%2C%20a%20denial%2Dof,host%20connected%20to%20the%20Internet.

10. Antivirus program [Electronic resource]: Access mode: URL: https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0
11. Internet security [Electronic resource]: Access mode: URL: https://en.wikipedia.org/wiki/Internet_security
12. Кибератака[Electronic resource]: Access mode: URL: https://www.cisco.com/c/ru_ru/products/security/common-cyberattacks.html
13. Basic methods of data protection [Electronic resource]: Access mode: URL: https://searchinform.ru/analitika-v-oblasti-ib/Issledovaniya-v-oblasti-ib/metody-obespecheniya-informatsionnoj-bezopasnosti/
14. Organizational means of information protection [Electronic resource]: Access mode: URL: https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/sposoby-zaschity-informatsii/

SIMULATION OF MOTION OF AN UNMANNED AERIAL VEHICLE FOR MEASURING PURPOSES AND PROTOTYPING OF ITS KINEMATIC DIAGRAM

Author: ***Oh Suchan***
Advisor: ***Leshkevich S.V.***
Belarus State University (Belarus)

Abstract. *The work is devoted to the development of an unmanned aerial vehicle, loaded with optical and radio measuring equipment, whose task is to identify and correct manufacturing defects in parts of wide-aperture antennas. The aim of the work is to create a simple, relatively autonomous aircraft with satisfactory aerodynamic qualities, the efficiency of which is ensured through the use of the latest achievements in electronics and radio communications. As the basis of the UAV, the Rogallo wing was used. To control the flight, a robot of the SCARA type was used, which ensured the parallel displacement of the steering trapezoid in the horizontal plane.*

Keywords: *unmanned aerial vehicle, flight control system, SCARA, Rogallo wing, microcontroller.*

I. INTRODUCTION

In areas such as space communications and radio astronomy, the received signals are extremely weak due to the large distances, so large apertures are needed to obtain sufficient signal energy. Typically a large aperture is implemented as a massive direct focus parabolic antenna that rotates mechanically. This somewhat outdated antenna architecture limits the use of parabolic antennas for many other applications. A more efficient antenna system design can improve the performance of all communication systems. With an increase in the aperture dimensions of the

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2021

Information Technology, Automation and Robotics

Proceedings

Odessa National Academy of Food Technologies

The collection includes student works of the participants of the competition, which were not included in the number of prize-winners. The texts of the competitive works are published in the form in which they were submitted by the authors. The authors of the articles are responsible for the content and form of submission of the material.

Responsible for the issue: Sergii Kotlyk

Computer typesetting and layout: Oksana Sokolova

Odessa 2021